John Foster Wallace
ZIMMERMAN & WALLACE
711 Gaffney Road, Suite 202
Fairbanks, AK 99701
(907) 452-2211
(907) 456-1137 facsimile
foster@mzwlaw.com
Attorney for Plaintiff Kendal L. Kaihoi

UNITED STATES DISTRICT COURT
DISTRICT OF ALASKA

KENDAL L. KAIHOI, individually and on behalf of all others similarly situated, *Plaintiff,* *v.* PREMERA, A Washington Non-Profit Corporation, and PREMERA BLUE CROSS, a Washington Non-Profit Corporation t/a and d/b/a PREMERA BLUE CROSS BLUE SHIELD OF ALASKA, *Defendants.*	**COMPLAINT – CLASS ACTION** **WITH JURY DEMAND** Case No. _____

Plaintiff Kendal L. Kaihoi, individually and on behalf of all others similarly situated, alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against PREMERA and Premera Blue Cross d/b/a and t/a Premera Blue Cross Blue Shield of Alaska (hereinafter collectively "Premera") for its failure to protect its members' confidential sensitive information-including their protected health information as defined by the Health Insurance Portability and Accountability Act

("HIPAA"), names, dates of birth, mailing addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information, and financial information (collectively, "Sensitive Information").

2. Premera is one of the largest health care insurance companies in the Pacific Northwest.

3. As a health care insurance provider, Premera is required to protect its members' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA.

4. In addition to its implied statutory obligation, Premera expressly promises - through its privacy policies and other written understandings - to safeguard and protect the confidentiality of its members' Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

5. Unfortunately, it took a massive medical data breach to reveal that Premera failed to provide its members' with the level of data protection that they were promised and for which they paid for.

6. Indeed, in March 2015, Premera confirmed that its computer network had been breached and that the Sensitive Information of approximately 11 million of its former and current members and employees were compromised.

7. Worse yet, according to Premera the breach started in May 2014 and went undetected for nearly one year. To make matters worse, after discovering the breach, Premera waited an additional month to notify affected members.

8. By maintaining its current and former members' Sensitive Information in electronic databases that lacked crucial security measures and industry standard data protections, Premera

jeopardized millions of its members' Sensitive Information and broke the paid-for promises and contractual obligations that it made to its members through its member agreements and privacy policies.

9. Unfortunately, as a result of Premera's failure to implement and follow these basic security procedures, Plaintiff s and the Class's Sensitive Information is now in the hands of unknown third parties.

PARTIES

10. Plaintiff Kendal L. Kaihoi is a natural person and citizen of the State of Alaska.

11. Defendant PREMERA is a nonprofit company organized and existing under the laws of the State of Washington. PREMERA is an upstream nonprofit holding company and the sole member of Premera Blue Cross.

12. Defendant Premera Blue Cross is a nonprofit company organized and existing under the laws of the State of Washington and domesticated in the State of Alaska. Premera Blue Cross conducts and transacts business in Alaska as Premera Blue Cross Blue Shield of Alaska. Premera Blue Cross has its principal place of business located at 7001 220th Street, SW, Building 1, Mount Lake Terrace, Washington 98043. Premera Blue Cross conducts business throughout this District, the State of Alaska, and the United States.

13. Currently and at all times relevant hereto, PREMERA was and is the parent company and sole member of Premera Blue Cross.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000 exclusive of interest and costs,

and (c) none of the exceptions under that subsection apply to this action.

15. This Court has personal jurisdiction over Defendant because Premera is domesticated in the District of Alaska, regularly conducts business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from this District.

16. Venue is proper pursuant to 28 U.S.C. § 139l(b) because Premera is domesticated in this District, and because the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from this District.

FACTUAL BACKGROUND

I. Premera's Privacy Policies Promised to Keep Members' Sensitive Information Confidential

17. Through its Notice of Privacy Practices (which all members receive), Premera represented that it would protect its members' Sensitive Information and keep it confidential. For instance, the Notice of Privacy Practices appearing on Premera's primary website and on Premera's Alaska specific website states, in relevant part:[1]

> **THE PRIVACY OF YOUR MEDICAL AND FINANCIAL INFORMATION IS VERY IMPORTANT TO US.**
>
> At Premera Blue Cross(Blue Shield of Alaska), we are committed to maintaining the confidentiality of your medical and financial information, which we refer to as your "personal information," regardless of format: oral, written, or electronic.
>
> * * *
>
> **OUR RESPONSIBILITIES TO PROTECT YOUR PERSONAL INFORMATION**
>
> Under both the Health Insurance Portability and Accountability Act of

[1] Premera Notice of Privacy Practices, https://www.premera.com/wa/visitor/privacy-policy/ (last visited May 5, 2015) and https://www.premera.com/ak/visitor/privacy-policy/ (Last visited on May 5, 2015).

> 1996 (HIPAA) and the Gramm-Leach-Bliley Act, Premera Blue Cross must take measures to protect the privacy of your personal information. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of your personal information include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.
>
> We protect your personal information in a variety of ways. For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of your information even if you no longer maintain coverage through us.
>
> We are required by law to:
>
> - protect the privacy of your personal information;
> - provide this Notice explaining our duties and privacy practices regarding your personal information;
> - notify you following a breach of your unsecured personal information; and
> - abide by the terms of this Notice.

18. In an additional document located on its primary website (Premera Blue Cross Code of Conduct 2014), Premera states:[2]

> We are committed to complying with federal and state privacy laws, including the HIPAA privacy regulations, that protect financial and health information of our customers. We use the following privacy principles to guide our actions:
>
> *Customers* - Customers should enjoy the full array of privacy protections afforded to them by law and routinely granted by their providers. This is a values-based approach whereby we are focused on two core values: Customer Care and Integrity.
>
> * * *
>
> We are committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' personal protected information (PPI).

[2] Premera Code of Conduct 2014, https://www.premera.com/documents/030553.pdf (last accessed May 8, 2015).

> We are expected to be aware of and follow established corporate policies, processes and procedures that are designed to secure our buildings and electronic systems. We are all responsible for maintaining the security of our campuses and buildings.

19. Premera's statements about its data security and management practices-both through its privacy policies and other public representations- served to falsely inflate the advertised utility of its insurance, thus allowing it and/or its affiliates to charge members higher costs for insurance and treatment. Specifically, Premera represented that it would take affirmative and commercially reasonable measures to protect consumers Sensitive Information and actively prevent disclosure and unauthorized access.

II. The Data Breach Revealed That Premera Failed to Properly Protect its Members' Sensitive Information.

20. In March 2015, Premera confirmed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [its] Information Technology (IT) systems."[3]According to Premera, approximately 11 million of its current and former members' (among others) names, dates of birth, email addresses, mailing addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, and claims information, including clinical information, were compromised as a result. The breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliate brands Vivacity and Connexion Insurance Solutions, Inc. The breach also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska.

21. According to Premera, the breach actually started in May 2014 and went undetected by it for nearly one year.[4]

[3] Premera Update, http://premeraupdate.com/ (last visited May 5, 2015).

[4] *Id* and by letter sent to Plaintiff and other class members from Premera dated March 17, 2015.

22. Worse still, after discovering the breach, Premera waited over one month to actually notify affected members. On March 17, 2015, Premera began notifying the public that it would be providing appropriate notification to affected members and regulatory agencies as required by federal and state law.

III. Premera Violated HIPAA and Industry Standard Data Protection Protocols.

23. HIPAA was enacted and became effective in 1996.

24. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services create rules to streamline the standards for handling Sensitive Information, like the data collected and stored in unsecure database(s) by Premera. The Department of Health and Human Services established standards to protect electronic personal health information from unauthorized disclosure. These standards require entities, such as Premera, to adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Sensitive Information.

25. Premera's data breach resulted from a variety of failures to follow HIPAA guidelines and industry standards. Among such deficient practices, Premera's breach shows that it failed to implement, or inadequately implemented, information security policies or procedures such as those requiring adequate intrusion detection systems, data encryption, and similar protection of Sensitive Information.

26. Premera's security failures demonstrate that it failed to honor its express and implied promises by failing to:

a. Maintain an adequate data security system to prevent data breaches;

b. Mitigate the risks of a data breach and unauthorized access to Sensitive Information;

c. Adequately encrypt or otherwise protect Plaintiff's and the Class's Sensitive Information;

d. Ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

e. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(l);

f. Implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(l);

g. Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(4); and

j. Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b).

27. Had Premera implemented proper security protocols to detect breaches *(i.e.*, detecting instances of unauthorized access to its databases) and to encrypt or otherwise protect its members' Sensitive Information, the consequences of the data breach would have been avoided (as it would have been detected nearly a year earlier and the damage could have been mitigated

and it would have also been virtually infeasible to extract its members' data). Worse yet, Premera knew or should have known that a security breach could result from its deficient security and privacy practices, as HIPAA and industry standard protections exist *specifically* to prevent unauthorized access to Sensitive Information.

28. Even though Premera members both expected and paid for the above-described security measures as part of their insurance premiums *(i.e.,* that HIPAA-mandated and industry standards would have been used to protect their Sensitive Information), they were not implemented, which resulted in the unsecured release of their Sensitive Information and the loss of paid-for data protection services.

IV. Plaintiff Kaihoi's Experience.

29. Plaintiff Kaihoi is a current member of Premera.

30. In order to purchase health insurance coverage from Premera, Kaihoi was required to provide Premera with his Sensitive Information in exchange for an agreement with Premera to receive health care insurance coverage and to protect his Sensitive Information in accordance with HIPAA, federal, state and local laws, and industry standards.

31. As such, Kaihoi paid Premera for medical insurance coverage and, among other things, the protection of his Sensitive Information.

32. Had Kaihoi known of Premera's substandard security procedures and method of protecting and storing his Sensitive Information, he would have paid substantially less for Premera's health insurance *(i.e.,* the value of health insurance *without* adequate protection of Sensitive Information is worth substantially less than the value of such insurance *with* adequate protection) or would not have paid at all *(i.e.,* he would not have purchased insurance from Premera in the first place).

33. Because Premera did not sufficiently protect his Sensitive Information, Kaihoi did not receive the entirety of the services he paid for and, as a result, he paid more than he otherwise would have for such services.

CLASS ALLEGATIONS

34. **Class Definition:** Plaintiff Kaihoi brings this action pursuant to Fed. R. Civ. P. 23(a), (b)(l), (b)(2), and (b)(3) on behalf of himself and a Class of similarly situated individuals, defined as follows:

> All persons in the United States and its territories (i) who paid money to Premera in exchange for health care insurance, and (ii) whose Sensitive Information was compromised as a result of the data breach confirmed by Premera in or around March 2015.

Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entity's current and former employees, officers, and directors, (2) the Judge to whom this case is assigned and the Judge's immediate family, (3) persons who execute and file a timely request for exclusion from the Class, (4) persons who have had their claims in this matter finally adjudicated and/or otherwise released, (5) Plaintiff's counsel and Defendant's counsel, and (6) the legal representatives, successors, and assigns of any such excluded person.

35. Awarding Plaintiff the declaratory and injunctive relief sought would necessarily affect the rights of all Class members. Further, the prosecution of separate lawsuits by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct for Defendant.

36. **Numerosity:** The exact number of members of the Class is unknown and is not available to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals. Class members can be easily identified through Defendant's records.

37. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

a) Whether Defendant took steps and measures to adequately safeguard Plaintiff s and the Class members' Sensitive Information;

b) Whether Defendant's storage of Plaintiff s and the Class members' Sensitive Information in the manner alleged violated industry standards, federal, state and local laws, and/or HIPAA;

c) Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and the members of the Class on the other;

d) Whether Defendant's conduct described herein constitutes a breach of its contracts with Plaintiff and the Class members; and

e) Whether Defendant should retain the monies paid by Plaintiff and other Class members to protect their Sensitive Information.

38. **Typicality:** Plaintiff s claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiff and the Class.

39. **Adequate Representation:** Plaintiff will fairly and adequately represent and

protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

40. **Policies Generally Applicable to the Class:** This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's practices challenged herein apply to and affect the Class members uniformly, and Plaintiff s challenge of those practices hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

41. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The injuries suffered by the individual members of the Class are likely to have been relatively small compared to the burden and expense of individual prosecution of the litigation necessitated by Defendant's actions. Absent a class action, it would be difficult, if not impossible, for the individual members of the Class to obtain effective relief from Defendant. Even if members of the Class themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties and the Court and require duplicative consideration of the legal and factual issues

presented herein. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION

Breach of Contract

(On behalf of Plaintiff and the Class)

42. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

43. Plaintiff and the Class members' paid money to Premera in exchange for its promise to provide health care insurance coverage.

44. In addition to providing health care insurance coverage, a material part of Premera's promise to provide coverage involved protecting Plaintiff s and the Class members' Sensitive Information.

45. In its written agreements as well as its privacy notices, Premera expressly promised Plaintiff and members of the Class that Premera only discloses health information when required to do so by federal or state law or with their consent. Premera further promised that it would protect their Sensitive Information.

46. Premera promised to comply with all HIPAA standards and to make sure that Plaintiff s and the Class members' Sensitive Information was protected. Premera further promised to provide notice to Plaintiff and members of the Class describing Premera's legal duties and privacy practices with respect to their Sensitive Information.

47. The contracts required Premera to safeguard Plaintiff s and the Class members' Sensitive Information to prevent its disclosure and/or unauthorized access.

48. Plaintiff and the Class members fully performed their obligations under the contracts.

49. Premera did not adequately safeguard Plaintiff's and the Class members' protected Sensitive Information. Specifically, Premera did not comply with its promise to comply with HIPAA's guidelines or industry standards when it stored its members' Sensitive Information.

50. The failure to meet these promises and obligations constitutes an express breach of contract. In other words, Premera breached the contracts with Plaintiff and the members of the Class by failing to implement sufficient security measures to protect Plaintiff's and the Class members' Sensitive Information as described herein.

51. Premera's failure to fulfill its data security and management promises resulted in Plaintiff and the Class members receiving services that were of less value than they paid for *(i.e.*, health care insurance coverage without adequate data security and management practices).

52. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive - even though such protections were a material part of their contracts with Premera - Plaintiff and the Class did not receive the full benefit of their bargain.

53. As a result of Premera's breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Premera's insurance as promised and the actual diminished value of its health care insurance.

SECOND CAUSE OF ACTION

Breach of Implied Contract

(in the alternative to Breach of Express Contract)

(On Behalf of Plaintiff and the Class)

54. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 40-51.

55. In order to benefit from Premera's insurance, Plaintiff and the Class disclosed

Sensitive Information to Premera, including their names, dates of birth, mailing addresses, telephone numbers, email addresses, Social Security numbers, medical information, and financial information.

56. By providing that Sensitive Information, and upon Premera' s acceptance of such information, Plaintiff and the Class, on the one hand, and Premera, on the other hand, entered into implied contracts whereby Premera was obligated to take reasonable steps to secure and safeguard that information.

57. Under the implied contract, Premera was further obligated to provide Plaintiff and the Class with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

58. Without such implied contracts, Plaintiff and the Class would not have provided their Sensitive Information to Premera.

59. As described herein, Premera did not take reasonable steps to safeguard Plaintiff s and the Class members' Sensitive Information.

60. Because Premera allowed unauthorized access to Plaintiff s and the Class members' Sensitive Information and failed to take reasonable steps to safeguard their Sensitive Information, Premera breached its implied contracts with Plaintiff and the Class.

61. The failure to meet these promises and obligations constitutes a breach of contract. In other words, Premera breached the contracts by failing to implement sufficient security measures to protect Plaintiff s and the Class members' Sensitive Information as described herein.

62. Premera's failure to fulfill its data security and management promises resulted in Plaintiff and the Class receiving services that were of less value than they paid for *(i.e.*, the

provision of health care insurance coverage without adequate data security and management practices).

63. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive-even though such protections were a material part of their contracts with Premera-Plaintiff and the Class did not receive the full benefit of their bargain.

64. As a result of Premera's breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Premera's insurance as promised and the actual diminished value of its health care insurance.

THIRD CAUSE OF ACTION

Restitution/Unjust Enrichment

(in the alternative to Counts I and II)

(On Behalf of Plaintiff and the Class)

65. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 40-62.

66. If the Court finds Plaintiff's and the Class members' contracts with Premera for protection of their Sensitive Information invalid, non-existent, or otherwise unenforceable, Plaintiff and the Class may be left without any adequate remedy at law.

67. Plaintiff and members of the Class conferred a monetary benefit on Premera in the form of fees paid for health care insurance coverage. Premera appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class.

68. The fees for health insurance that Plaintiff and the Class paid to Premera were supposed to be used by Premera, in part, to pay for the administrative costs of data management and security.

69. Under principles of equity and good conscience, Premera should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Premera failed to implement data management and security measures that Plaintiff and the Class paid for and are otherwise mandated by HIPAA and industry standards.

70. Accordingly, as a result of Premera's conduct, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Premera's insurance as promised and the actual diminished value of the health care insurance received.

FOURTH CAUSE OF ACTION

Failure to Timely Disclose Breach Under Alaska Personal Information Act

AS 45.48.010 - AS 45.48.090

(On Behalf of Plaintiff and the Class)

71. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

72. Premera is a corporation operating in Alaska that owns or licenses personal information of Alaska residents as that term is defined in AS 45.48.090(7).

73. On or about May 5, 2014 unauthorized individuals acquired personal information of Alaska residents from Premera that compromises the security, confidentiality, or integrity of the personal information maintained by Premera.

74. Premera knew or should have known that the breach occurred, but due to its own negligent monitoring of its information technology system containing the personal information of Alaska residents, it did not discover the breach until January 29, 2015.

75. Premera did not notify each Alaska resident whose personal information was subject to the breach until a letter was sent on March 17, 2015.

76. Premera's failure to disclose the breach to the Alaska residents until more than

ten months after the breach occurred, and more than six weeks after the breach was allegedly discovered, was not disclosed in the most expeditious time possible and constituted unreasonable delay.

77. As a direct and proximate result of Premera's failure to provide disclosure of the breach as required by Alaska law, Plaintiff and the class have suffered damages.

FIFTH CAUSE OF ACTION

Failure to Timely Disclose Breach Under RCW 19.255.010

(On Behalf of Plaintiff and the Class)

78. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

79. Premera is a business that conducts business in the State of Washington and that owns or licenses computerized data that includes personal information, as that term is defined in RCW 19.255.010.

80. On or about May 5, 2014, unauthorized users gained access to Premera's information technology systems, breaching the security of the information technology system that stored personal information. Premera allowed an unauthorized acquisition of computerized data that compromised the security, confidentiality, or integrity of personal information maintained by Premera.

81. Premera knew or should have known that the breach occurred, but due to its own negligent monitoring of its information technology systems containing personal information, did not discover the breach until January 29, 2015.

82. Premera did not notify the persons whose data was breached of the data breach until March 17, 2015.

83. Premera's failure to disclose the breach of the security of the system storing personal information until more than ten months after the breach occurred, and more than six weeks after the breach was purportedly discovered, constituted unreasonable delay and was not a disclosure in the most expedient time possible.

84. As a direct and proximate result of Premera's failure to provide reasonably prompt disclosure, Plaintiff and the Class have suffered damages.

REQUEST FOR RELIEF

Plaintiff Kendal L. Kaihoi, on behalf of himself and the Class, respectfully requests that this Court enter an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Kaihoi as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Premera's actions, as described above, constitute (i) breach of express contract, (ii) breach of implied contract (in the alternative to breach of express contract), (iii) unjust enrichment (in the alternative to breach of express contract and breach of implied contract), a violation of the Alaska Personal Information Act; and (iv) a violation of the Washington State law, specifically, RCW 19.255.010;

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Premera from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Premera to protect all data collected through the course of its business in accordance with HIPAA, and (iv) industry standards;

D. Awarding damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding restitution to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

DATED at Fairbanks, Alaska, this 13th day of May, 2015.

By:*/s/ John Foster Wallace*

John Foster Wallace, ABA#9211115
ZIMMERMAN & WALLACE
711 Gaffney Road, Suite 202
Fairbanks, AK 99701
(907) 452-2211
(907) 456-1137 fax
foster@mzwlaw.com

David S. Senoff, Esquire*
CAROSELLI BEACHLER McTIERNAN & COLEMAN, LLC
1845 Walnut Street, Fifteenth Floor
Philadelphia, PA 19103
(215) 609-1350
(215) 609-1351 fax
dsenoff@cbmclaw.com

*Admission *pro hac vice* to be sought.